SC&H GROUP

Expertise that Works

IT RISK ASSESSMENTS ENHANCE OPERATIONAL EFFICIENCIES AND BUSINESS OUTCOMES

SCOTT HEFLIN, PRINCIPAL, SC&H GROUP RISK MANAGEMENT PRACTICE

Information Technology (IT) has become the foundation for virtually every business across the globe. Whether for supply chain management or for new mobility and bring-your-own-device (BYOD) efforts, IT drives efficiencies and business outcomes on many levels.

By being dependent on IT, there are many inherent business risks that organizations should consider, which is why IT Risk Assessments play a major role in ensuring that technology truly supports business goals and objectives.

Following is a Q&A interview with Scott Heflin, a Principal in the SC&H Group Risk Management practice, who provides an overview of IT risk and why Risk Assessments are vital to any organization.

Q: **What is IT risk?**

A: By definition, IT risk is business risk – specifically with the use, ownership, operation, and adoption of IT within an enterprise. It consists of any IT-related events and conditions that could potentially impact the business, and prevent the enterprise from meeting its strategic goals and objectives.

Q: **Why is an assessment of IT risk important?**

A: Risk Assessments, whether they pertain to IT or other types of risk, are a means of providing decision-makers with the information needed to understand factors that can negatively influence operations.

These assessments can help predict potential outcomes and provide informed judgments concerning the extent of actions needed to reduce the identified risks. As reliance on computer systems and electronic data has grown, IT risk has joined the array of risks that all businesses must manage to ensure the enterprise successfully meets strategic goals and objectives. Most people understand that IT innovation creates opportunities, but far too often they overlook the associated risks.

Q: **What are the benefits of an IT Risk Assessment?**

A: There are numerous benefits of an IT Risk Assessment. As I mentioned, it provides decision-makers with a better understanding of how their operations could be negatively affected by their use of IT. An organization that fully understands the IT-related risks facing the company typically has less IT service interruptions, is better positioned to identify and avoid security vulnerabilities, experiences fewer compliance issues, and is more successful in enabling technology for new business initiatives and more efficient operations.

Q: **Who should have an IT Risk Assessment performed?**

A: Every organization that uses IT systems as part of their daily operations should be conducting IT Risk Assessments. The management of business risks is an essential component of the responsible administration of any enterprise. It should be noted, however, that the frequency and scope of the assessment will vary depending on the complexity of the IT environment and the degree to which it is being leveraged by the organization.

Q: **How is a typical IT Risk Assessment conducted?**

A: The typical IT Risk Assessment process consists of interviews with key IT and business personnel, observation of the facilities, and an examination of supporting documentation – such as system inventory listings, network diagrams, IT and business process policies and procedures, etc.

Based on the interviews and data gathering, there are then a number of steps performed throughout the process which include identifying the business objectives, current IT threats, and current vulnerabilities; analyzing existing and planned IT controls in place; determining the likelihood and impact ratings for all identified risks; assigning overall risk rankings; and ultimately organizing and documenting the results into the desired reporting format.

Q: **Who are the key participants of the IT Risk Assessment process?**

A: Many people incorrectly assume that the IT Risk Assessment process is a technical function carried out solely by the IT experts who operate and manage the IT systems. IT is an essential management function of the organization; therefore a successful IT Risk Assessment requires the full support and participation from senior management, IT Administrators, and functional managers of the business. This combination ensures that the IT Risk Assessment process will help protect the organization and its ability to perform their mission, not just its IT assets.

While some organizations may elect to perform the IT Risk Assessments internally, using consulting expertise beyond the boundaries of the organization provides additional benefits because of their objectivity and broader exposure experience. This is exactly where SC&H Group can help.

Q: **How long does a typical IT Risk Assessment project take?**

A: The scope of an IT Risk Assessment project will vary depending on the size and complexity of the organization and its IT environment, as well as the degree to which IT is being utilized within the enterprise. The level of effort required to complete the project is different for each organization.

Q: How often does an IT Risk Assessment need to be performed?

A: Certainly as business operations, workflow, or technologies change, periodic reviews should be conducted to analyze the changes, account for new threats and vulnerabilities created by the changes, and determine the effectiveness of existing controls. While a full-scale IT Risk Assessment may not be required each year, it is recommended that organizations do a review and "refresh" of their IT Risk Assessment results on an annual basis.

ABOUT SCOTT HEFLIN *As a Principal in the SC&H Group Risk Management practice, Scott is an accomplished Information Technology audit and advisory professional with more than 13 years of experience. He helps organizations to identify and respond to IT-related risks, strengthen internal controls, and improve compliance and operational performance. Scott is both a Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM). He also holds certifications in Risk and Information Systems Control (CRISC), and Risk Management Assurance (CRMA).*

ABOUT SC&H GROUP *SC&H Group is an audit, tax, and consulting firm applying "expertise that works" to minimize risk and maximize value. SC&H Group's practices advise leading companies from emerging businesses to the Fortune 500 on accounting, tax, profitability and strategy solutions. Clients in all states and worldwide benefit from SC&H Group's commitment to delivering powerful minds, passionate teams, and proven results on each and every engagement. Learn more at* **www.scandh.com**.

POWERFUL MINDS | PASSIONATE TEAMS | PROVEN RESULTS

Visit | www.scandh.com **Toll Free** | 800-921-8490 **Email** | sch_consulting@scandh.com